A. The Present Invention

The present invention discloses an extended X.509 certificate capable of supporting more than one cryptographic algorithm. The certificate comprises a signature algorithm and a signature for all authenticated attributes using a first cryptographic algorithm, and alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key, and an alternative signature extension for containing a signature for the alternative cryptographic algorithm.

B. Differences Between the Present Claims and the Cited Art

The Office Action identifies a passage from Shambroom as disclosing "a certificate that supports one or more cryptographic algorithms" and that "the certificate can resemble an X.509 certificate," citing Column 10, lines 32-35

More specifically, Shambroom states that "web server 720 responds with a certificate to web browser 620. This certificate contains the network server's public key and a list of one or more cryptographic algorithms that the network server supports..." (Column 10, lines 30-34).

The key here is that the Shambroom certificate contains a **list** of one or more cryptographic algorithms that the **network server** supports. The Shambroom certificate does not actually use or employ multiple cryptographic algorithms to protect the data therein. The Shambroom data appears to be the list of algorithms. The certificate in Claim 1 does **not** contain a list of cryptographic algorithms that a network server supports. The claimed certificate utilizes and uses more than one cryptographic algorithm itself to protect the data it includes.

Further, the network server's public key appears to be used by the web browser to log onto or communicate with the web server 720, which is part of the network server 700, and not to protect the data in the certificate. In other words, the Shambroom certificate is used to transfer

data, including the list of cryptographic algorithms that the network server supports and the public key for the network server, to the web browser. No such scheme is contemplated by the present invention.

Claim 1 recites that the X.509 certificate comprises "a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;" as well as "an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and an alternative signature extension for containing a signature for the alternative cryptographic algorithm." This is not the same thing as a list of cryptographic algorithms that a network server supports as per Shambroom, and such a list included in a certificate does not teach, suggest or disclose the subject matter of Claim 1. Shambroom does not teach that its certificate protects its data using more than one cryptographic algorithm. The Shambroom list appears to be data included in the certificate, not multiple cryptographic algorithms employed by the certificate to protect its data, as per Claim 1.

Schneier appears to describe a standard X.509 certificate which employs a single cryptographic algorithm. Applicant notes that portions of pages 480, 481, 574 and 575 of Schneier were not legible in the photocopies provided with the Office Action.

Including a list of cryptographic algorithms as data in a certificate does not teach, suggest or disclose using multiple algorithms to protect the data in the certificate. There is not reason to combine Shambroom's list of cryptographic algorithms contained in a certificate (which indicate which algorithms a server supports) with the standard X.509 certificate, such as that of Schneier, which actually uses a single algorithm to protect data contained therein.

Finally, neither Shambroom nor Schneier discusses the use of extensions to enable the certificate to support an alternative cryptographic algorithm, as per the second and third elements of Claim 1.

Accordingly, Applicant submits that Claim 1 patentably distinguishes over the combination of Shambroom and Schneier. Accordingly, dependent Claim 2 and 3 should also distinguish over the cited art.

II. Object to the Drawings

Applicant is submitting herewith a proposed drawing correction to obviate the objection to the drawings.

II Summary

Applicant has presented technical explanations and arguments fully supporting their position that the pending claims contain subject matter which is not taught, suggested or disclosed by Shambroom, Schneier, or any combination thereof. Accordingly, Applicant submits that the present Application is in a condition for Allowance. Reconsideration of the claims and a Notice of Allowance are earnestly solicited.

Respectfully submitted,

Gregory M. Doudnikoff
Attorney for Applicant
Reg. No. 32,847

GMD/lld

Docket No: CR9-98-095
PHONE: 919-254-1288
FAX: 919-254-4330